(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 June 2005 (23.06.2005)

PCT

(10) International Publication Number
WO 2005/057382 A1

(51) International Patent Classification[7]: G06F 1/00, H04L 29/06

(21) International Application Number: PCT/CH2004/000734

(22) International Filing Date: 13 December 2004 (13.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03405896.6 15 December 2003 (15.12.2003) EP

(71) Applicant *(for all designated States except US)*: **ABB RESEARCH LTD** [CH/CH]; Affolternstrasse 52, CH-8050 Zürich (CH).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NAEDELE, Martin** [DE/CH]; Neunbrunnenstrasse 90, CH-8050 Zürich (CH). **BIDERBOST, Oliver** [CH/CH]; Hofacherstrasse 5, CH-8624 Grüt (CH).

(74) Agent: **ABB SCHWEIZ AG**; Intellectual Property (CH-LC/IP), Brown Boveri Strasse 6, CH-5400 Baden (CH).

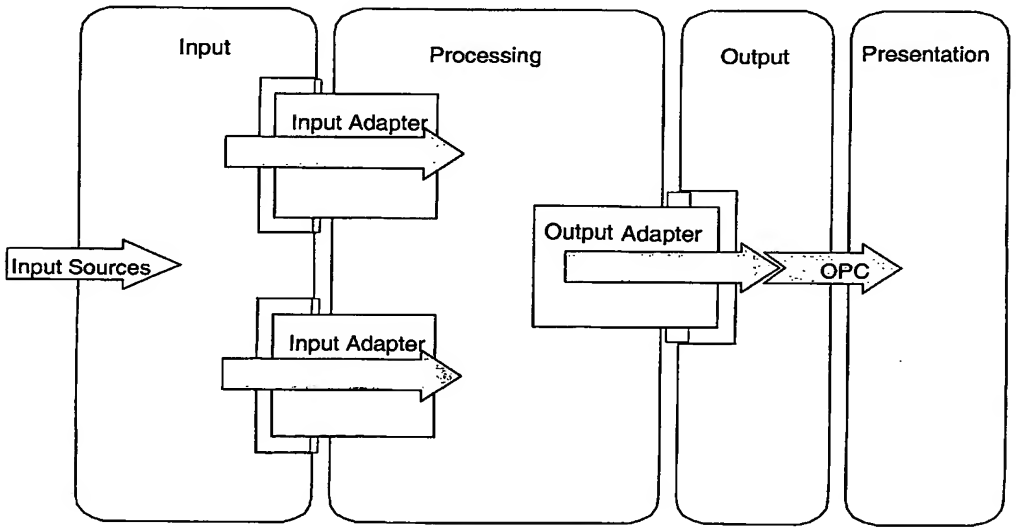
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: NETWORK SECURITY SYSTEM



(57) Abstract: The inventive IT Security System for intrusion detection in a private network, which is connected to a public network, comprises a processing system, a supervisory system and an interface system. The processing system detects intrusion or unwanted access of resources on a private network and alerts in case of a detected intrusion or unwanted access of resources by creating quantitative alert data. The supervisory system automatically processes the alerts or presents the alerts to a security system operator. The interface system transfers the alerts from the processing system to the supervisory system. Available data about network activity can thus be presented to the operator in an intuitive and non-technical manner. If the operator suspects the security of the network to be compromised he can safely isolate the private network from the outside world, as simple reaction to any threat endangering the private network environment.

WO 2005/057382 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.